UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

| APPLICATION NO. | FILING DATE | FIRST NAMED INVENTOR | ATTORNEY DOCKET NO. | CONFIRMATION NO. |
|---|---|---|---|---|
| 09/625,817 | 07/26/2000 | Daniel Bleichenbacher | BLEICHENBACHER 4-27 | 8285 |

47394 7590 01/30/2006

HITT GAINES, PC
LUCENT TECHNOLOGIES INC.
PO BOX 832570
RICHARDSON, TX 75083

| EXAMINER | |
|---|---|
| WINDER, PATRICE L | |

| ART UNIT | PAPER NUMBER |
|---|---|
| 2145 | |

DATE MAILED: 01/30/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

| Office Action Summary | Application No. | Applicant(s) | |
|---|---|---|---|
| | 09/625,817 | BLEICHENBACHER ET AL. | |
| | Examiner | Art Unit | |
| | Patrice Winder | 2145 | |

*-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --*

**Period for Reply**

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

**Status**

1)☒ Responsive to communication(s) filed on *31 October 2005*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

**Disposition of Claims**

4)☒ Claim(s) *1-14* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-14* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

**Application Papers**

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *26 July 2000* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

**Priority under 35 U.S.C. § 119**

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

**Attachment(s)**

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

## DETAILED ACTION

### *Response to Arguments*

1. Applicant's arguments, see page 2 of the Remarks/Arguments, filed February 22, 2005, with respect to the rejection(s) of claim(s) 1-14 under 103(a) have been fully considered and are persuasive. Therefore, the rejection has been withdrawn. However, upon further consideration, a new ground(s) of rejection is made in view of Aura and Trostle.

### *Claim Rejections - 35 USC § 103*

2. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

3. This application currently names joint inventors. In considering patentability of the claims under 35 U.S.C. 103(a), the examiner presumes that the subject matter of the various claims was commonly owned at the time any inventions covered therein were made absent any evidence to the contrary. Applicant is advised of the obligation under 37 CFR 1.56 to point out the inventor and invention dates of each claim that was not commonly owned at the time a later invention was made in order for the examiner to consider the applicability of 35 U.S.C. 103(c) and potential 35 U.S.C. 102(e), (f) or (g) prior art under 35 U.S.C. 103(a).

4. Claims 1-14 are rejected under 35 U.S.C. 103(a) as being unpatentable over Tuomas Aura et al., DOS-resistant Authentication with Client Puzzles (hereafter referred to as Aura) in view of Trostle, USPN 5,919,257 (hereafter referred to as Trostle).

5. Regarding claim 1, Aura taught a system for controlling access to a resource of a computer system (column 2, lines 45-53), comprising:

a database of problems (page 5, "The server stores the values C, $N_s$ $N_c$ as long as it still considers the nonce $N_s$ recent.");

a problem retriever that responds to a request from a client for access to said resource by retrieving one of said problems and transmitting said one of said problems to said client (page 4, "To create new puzzles, the server periodically generates a nonce Ns and sends it to client. "), and

a solution evaluator that, upon receiving a putative solution from said client, validates said putative solution and, if said putative solution is valid, grants said client access to said resource (page 5, "The server verifies the client's solution to the puzzle by computing the hash and, only after seeing that it is correct verifies the signature and continues with the last message of the authentication."). Aura does not specifically teach the database including corresponding pre-calculated solutions and employing said database. However, Trostle taught a database including corresponding pre-calculated solutions and employing the database (column 7, lines 3-10). It would have been obvious to one of ordinary skill in the art at the time the invention was made that incorporating Trostle's database of pre-calculated solutions in Aura's protocol for providing DOS-resistant authentication would have been an equivalent mechanism for

providing solution verification. The motivation would have been because a desirable alternative to performing the hash function is to lookup the hash values in a database.

6. Regarding dependent claim 2, Aura taught said problems comprise outputs and portions of corresponding inputs to a one-way function (page 3, "The puzzle we use is the brute- force reversal of a one-way function such as MD5 or SHA.").

7. Regarding dependent claim 3, Aura taught said one-way function is a Message Digest-5 function (page 3, "The puzzle we use is the brute- force reversal of a one-way function such as MD5 or SHA").

8. Regarding dependent claim 4, Aura taught said problem retriever replaces said one of said problems and a corresponding one of said solutions when said putative solution is valid (page 5, "The server verifies the client's solution to the puzzle by computing the hash and, only after seeing that it is correct verifies the signature and continues with the last message of the authentication.").

9. Regarding dependent claim 5, Aura taught said problem retriever replaces said one of said problems and a corresponding one of said solutions only when said putative solution is valid (page 5, "The server verifies the client's solution to the puzzle by computing the hash and, only after seeing that it is correct verifies the signature and continues with the last message of the authentication.").

10. Regarding dependent claim 6, Aura taught said solution evaluator grants said client access to said resource by allocating memory associated with said resource to serve said client (page 1, "In this paper, we advocate the design principle that *the client*

*should always commit its resources to the authentication protocol first and the server should be able to verify the client commitment before allocating its own resources.*").

11. Regarding dependent claim 7, Aura taught said resource is selected from the group consisting of: a network server (page 1, "In this paper, we advocate the design principle that *the client should always commit its resources to the authentication protocol first and the server should be able to verify the client commitment before allocating its own resources.*"), an electronic mail server, and a main database.

12. The language of claims 8-14 is substantially the same as previously rejected claims 1-7. Therefore, claim 8-14 are rejected on the same rationale as previously rejected claims 1-7, supra.

***Conclusion***

13. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

14. Rose et al., USPN 6,944,765: a method of enabling a provider to authenticate users including the steps of constructing a in response to information received from user, sending to the user; and returning a solution to the puzzle to the provider.

15. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Patrice Winder whose telephone number is 571-272-3935. The examiner can normally be reached on Monday-Friday, 10:30 am-7:00 pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Jason Car done can be reached on 571-272-3933. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Patrice Winder
Primary Examiner
Art Unit 2145

January 20, 2006